

REMARKS

Claims 1-20 are pending in this application. By this Amendment, claims 1-18 are amended to merely clarify the recited subject matter, and new claims 19-20 are introduced to protect additional aspects of the invention. No new matter is added by this Amendment because the claim amendments and new claims are fully supported by the originally filed specification and claims.

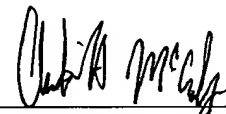
Attached hereto is a marked-up version of the changes made to the claims by the current Amendment. The attached Appendix is captioned "VERSION WITH MARKINGS TO SHOW CHANGES MADE".

Prompt examination and favorable consideration on the merits are respectfully requested.

Respectfully submitted,

PILLSBURY WINTHROP LLP

By: _____



Christine H. McCarthy
Reg. No. 41,844
Tel. No.: (703) 905-2143
Fax No.: (703) 905-2500

CHM/AM

1600 Tysons Boulevard
McLean, VA 22102
(703) 905-2000

Enclosure: Appendix

APPENDIX

VERSION WITH MARKINGS TO SHOW CHANGES MADE

IN THE TITLE:

Please delete the pending title and replace it with the following title: --ARRANGING AUTHENTICATION AND CIPHERING IN MOBILE COMMUNICATION SYSTEMS--.

IN THE CLAIMS:

1. (Amended) A method of arranging data protection in a telecommunication system [comprising] including a first mobile communication network [wherein a first cipher key is used for ciphering traffic between a mobile station and a mobile communication network], a second mobile communication network [wherein a second cipher key is used for ciphering traffic between a mobile station and a mobile communication network], and a mobile station supporting both of [said] the mobile communication networks, [**c h a r a c t e r i z e d** by] the method comprising:

ciphering traffic between the mobile station and the first mobile communication network using a first cipher key;

calculating [said] a second cipher key to be used for ciphering traffic between the mobile station and the second mobile communication network in the first mobile communication network when the mobile station operates in the first mobile communication network[.];

transmitting information necessary for calculating [said] the second cipher key from the first mobile communication network to the mobile station when the mobile station operates in the first mobile communication network[.]; and

calculating [said] the second cipher key at the mobile station to be used for ciphering traffic between the mobile station and the second mobile communication network.

2. (Amended) [A method as claimed in] The method of claim 1,
[c h a r a c t e r i z e d by] further comprising:

[using said second cipher key for] ciphering the traffic between the mobile station and the second mobile communication network using the second cipher key if the mobile station is handed over from the first mobile communication network to the second mobile communication network during an active connection.

3. (Amended) [A method as claimed in] The method of claim 1,
[c h a r a c t e r i z e d by] further comprising:

transmitting [said] the second cipher key from the first mobile communication network to the second mobile communication network[,];

transmitting [said] the second cipher key calculated at the mobile station to a ciphering [means] module of the mobile station in response to [the fact that the first mobile communication network transmits a request to the mobile station for handover to the second mobile communication network] a request from the first mobile communication network to handover to the second mobile communication network; and

[using said second cipher key in] ciphering traffic [after the handover in the mobile station and in the second mobile communication network] between the mobile station and the second mobile communication network using the second cipher key after handover is complete.

4. (Twice Amended) [A method as claimed in] The method of claim 1,
[c h a r a c t e r i z e d by] further comprising:

[checking] determining, in the first mobile communication network, whether the mobile station supports the second mobile communication network;[,]

calculating [said] the second cipher key in the first mobile communication network in response to [the fact that] a determination that the mobile station supports the second mobile communication network;[,]

transmitting a request for calculation of [said] the second cipher key from the first mobile communication network to the mobile station[,]; and

calculating [at the mobile station said] the second cipher key at the mobile station in response to [said] the request for calculation of the second cipher key.

5. (Amended) [A method as claimed in] The method of claim 4,
[c h a r a c t e r i z e d by] wherein [calculating said] the second cipher key is calculated in the first mobile communication network [in response to the fact that] when an identifier transmitted by the mobile station[, such as an IMSI subscriber identifier, and/or a classmark identifier indicate] indicates that the mobile station supports the second mobile communication network.

6. (Twice Amended) [A method as claimed] The method of claim 1,
[c h a r a c t e r i z e d by] further comprising:

calculating [said] the second cipher key at a [network] first element in the first mobile communication network[, such as an authentication centre,] in response to [the fact that a network element of the first mobile communication network, such as a visitor location register or a home location register, comprising identifiers transmitted by the mobile station requests calculation of said second cipher key] a request from a second element of the first

mobile communication network, the second element including identifiers transmitted by the mobile station, and

transmitting [said] the second cipher key from [said network] the first element [calculating the cipher key] to [said] the second [network] element [comprising the identifiers transmitted by the mobile station].

7. (Twice Amended) [A method as claimed in] The method of claim 1,
[c h a r a c t e r i z e d by] wherein the mobile station [comprising] includes a [subscriber identification] USIM application[, such as a USIM application, to] for the first mobile communication network and a subscriber identification SIM application[, such as an SIM application, to] for the second mobile communication network, the method further comprising:

transmitting [the] information necessary [for calculating said] to calculate the second cipher key received by the mobile station to the [identification] SIM application [according to the second mobile communication network].

8. (Twice Amended) [A method as claimed in] The method of claim [1] 7,
[c h a r a c t e r i z e d by] further comprising:

calculating [said] the second cipher key in the first mobile communication network in connection with calculating an authentication response [according to] for the first mobile communication network and the first cipher key[.,];

transmitting the information necessary for calculating the first cipher key and [said] the second cipher key, such as a random-number parameter, from the first mobile communication network to the mobile station[.,];

transmitting the necessary information [at the mobile station] for calculating [said] the first and second cipher keys from the mobile station to the subscriber identification applications [according to] for the first and the second mobile communication networks[,];

calculating [said] the second cipher key in the subscriber identification application [according to] for the second mobile communication network and calculating the authentication response in the subscriber identification application [according to] for the first mobile communication network[,];

transmitting [said] the authentication response [according to] for the first mobile communication network from the mobile station to the first mobile communication network[,]; and

acknowledging the authentication of the mobile station [to be performed for] in the second mobile communication network in response to [the fact that] the first mobile communication network [accepts] accepting the authentication response transmitted by the mobile station.

9. (Twice Amended) [A method as claimed in] The method of claim [1] 7,
[c h a r a c t e r i z e d b y] further comprising:

determining a random-number parameter and calculating [the] an authentication response [according to] for the second mobile communication network in connection with calculating [said] the second cipher key in the first mobile communication network[,];

transmitting a request [to the mobile station] for [calculation of an] calculating an authentication response [according to] for the second mobile communication network to the mobile station[,];

transmitting the information necessary [at the mobile station] for calculating [said] the second cipher key from the mobile station to the subscriber identification SIM application [according to the second mobile communication network];[,]

calculating[, in the identification application according to the second mobile communication network,] the authentication response [according to] for the second mobile communication network in connection with calculating said second cipher key using the subscriber identification SIM application module;[,]

transmitting the authentication response [according to] for the second mobile communication network that is calculated at the mobile station to the first mobile communication network[,]; and

checking said authentication response according to the second mobile communication network transmitted by the mobile station in the first mobile communication network.

10. (Twice Amended) [A method as claimed in] The method of claim 1, [c h a r a c t e r i z e d by] wherein[calculating said] the second cipher key is calculated by shortening the first cipher key in the first mobile communication network, and at the mobile station before [the] a handover to the second mobile communication network takes place.

11. (Twice Amended) [A method as claimed in] The method of claim 1, [c h a r a c t e r i z e d by] wherein [calculating said] the second cipher key is calculated in response to [the fact that a decision has been made in the first mobile communication network] a decision in the first mobile communication network to carry out a handover to the second mobile communication network.

12. (Amended) A telecommunication system comprising: [at least]

a first mobile communication network [arranged] configured to use a first cipher key for ciphering traffic between a mobile station and [a] the first mobile communication network;₁[,]

a second mobile communication network [arranged] configured to use a second cipher key for ciphering traffic between a mobile station and [a] the second mobile communication network;₂[,] and

a mobile station [arranged] configured to support said different first and second mobile communication networks, [**c h a r a c t e r i z e d** in that]

wherein the first mobile communication network is [arranged] configured to calculate [said] the second cipher key when the mobile station operates in the first mobile communication network, and the first mobile communication network is [arranged] configured to transmit information necessary for calculating [said] the second cipher key from the first mobile communication network to the mobile station when the mobile station operates in the first mobile communication network, and the mobile station is [arranged] configured to calculate said second cipher key.

13. (Amended) [A] The telecommunication system [as claimed in] of claim 12, [**c h a r a c t e r i z e d** in that] wherein the mobile station and the second mobile communication network are [arranged] configured to cipher [the] traffic between the mobile station and the second mobile communication network [by] using [said] the second cipher key if the mobile station is handed over from the first mobile communication network to the second mobile communication network during an active connection.

14. (Twice Amended) [A] The telecommunication system [as claimed in] of claim 12, [**c h a r a c t e r i z e d** in that] wherein

the first mobile communication network is [arranged] configured to transmit [said] the second cipher key to the second mobile communication network before [the] a handover to the second mobile communication network,

the mobile station is [arranged] configured to transmit said second cipher key calculated at the mobile station to a ciphering means of the mobile station in response to [the fact that] the first mobile communication network [transmits] transmitting a request to the mobile station for handover to the second mobile communication network, and

the mobile station and the second mobile communication network are [arranged] configured to cipher [use said second cipher key in ciphering] traffic after the handover using the second cipher key.

15. (Twice Amended) [A] The telecommunication system [as claimed in any one] of claim 12, [c h a r a c t e r i z e d in that] wherein

the first mobile communication network is [arranged] configured to [check] determine whether the mobile station supports the second mobile communication network based on [the basis of] an identifier transmitted by the mobile station[, such as an IMSI and/or a classmark identifier],

the first mobile communication network is [arranged] configured to calculate [said] the second cipher key in response to [the fact] a determination that the mobile station supports the second mobile communication network,

the first mobile communication network is [arranged] configured to transmit a request to the mobile station for calculation of [said] the second cipher key, and

the mobile station is [arranged] configured to calculate said second cipher key based on the [basis of said] request from the first mobile communication network.

16. (Twice Amended) [A] The telecommunication system [as claimed in] of claim 12, [c h a r a c t e r i z e d in that] further comprising:

a first element of the first mobile communication network configured to receive the request for calculation of the second cipher key from a second [network] element [comprising] of the first mobile communication network configured to store identifiers transmitted by the mobile station of the first mobile communication network[, such as a visitor location register or a home location register, is arranged to transmit the request for calculation of said second cipher key to a network element of the first mobile communication network, such as an authentication centre],

wherein the first [network] element [of the first mobile communication network, such as the authentication centre,] is [arranged] configured to calculate [said] the second cipher key in response to [the fact that the network element comprising the identifiers transmitted by the mobile station requests calculation of said second cipher key] the request from the second element, and[said] the first [network] element [calculating said second cipher key] is [arranged] configured to transmit the calculated second cipher key to [said] the second [network] element [comprising the identifiers transmitted by the mobile station].

17. (Twice Amended) [A] The telecommunication system [as claimed in] of claim 12, [c h a r a c t e r i z e d in that] wherein

the first mobile communication network is [arranged] configured to calculate [said] the second cipher key in connection with calculation of an authentication response [according to] associated with the first mobile communication network and the first cipher key,

the first mobile communication network is [arranged] configured to transmit to the mobile station information necessary for calculating the first cipher key and [said] the second cipher key, such as a random-number parameter,

the mobile station [comprises] includes [an] a USIM identification application [according to] for the first mobile communication network[, such as a USIM application,] and [an] a SIM identification application [according to] for the second mobile communication network, [such as an SIM application,]

the mobile station is [arranged] configured to transmit [said] the information necessary for calculating the first cipher key and [said] the second cipher key to the identification applications [according to] for the first and the second mobile communication networks,

[said] the SIM identification application [according to the second mobile communication network] is [arranged] configured to calculate [said] the second cipher key, [and]

[said] the USIM identification application [according to the first mobile communication network] is [arranged] configured to calculate the authentication response [according to] for the first mobile communication network, and

the mobile station is [arranged] configured to transmit the authentication response [according to] for the first mobile communication network to the first mobile communication network.

18. (Twice Amended) [A] The telecommunication system [as claimed in] of claim12, [c h a r a c t e r i z e d in that] wherein

the first mobile communication network is [arranged] configured to determine a random-number parameter [according to] for the second mobile communication network and to calculate the authentication response in connection with calculating [said] the second cipher key,

the first mobile communication network is [arranged] configured to transmit a request to the mobile station [for calculating the] to calculate an authentication response [according to] for the second mobile communication network,

the mobile station [comprises] includes a USIM [an] identification application [according to] for the first mobile communication network[, such as a USIM application,] and [an] a SIM identification application [according to] for the second mobile communication network[, such as an SIM application],

the mobile station is [arranged] configured to transmit the information necessary [for calculating said] to calculate the second cipher key to the SIM identification application [according to] for the second mobile communication network,

the SIM identification application [according to] for the second mobile communication network is [arranged] configured to calculate [said] the second cipher key and the authentication response [according to] for the second mobile communication network substantially simultaneously,

the mobile station is [arranged] configured to transmit the authentication response [according to] for the second mobile communication network to the first mobile communication network, and

the [second] first mobile communication network is [arranged] configured to check the authentication response [according to] for the second mobile communication network.